Hoja de datos de servicios

Servicio de administración de operaciones de seguridad

Excelencia operativa para operaciones de seguridad y respuesta a incidentes

En resumen

- Implemente procesos y procedimientos de administración de servicios y seguridad para lograr una administración eficiente de incidentes y operaciones de seguridad.
- Identifique los procesos existentes para automatizarlos.
- Defina e implemente procedimientos y manuales de ejecución operativos completos.
- Identifique informes clave y vistas de tablero para automatización.
- Mejore la eficiencia y la automatización de las operaciones de seguridad en toda la empresa.

Con el aumento de las amenazas de seguridad externas e internas, y el incremento de los incidentes de seguridad, las organizaciones están mejorando las operaciones de seguridad y los métodos y los procedimientos de respuesta a incidentes para aplicar inteligencia que les permita desviar de manera proactiva las amenazas de seguridad y aumentar la capacidad de respuesta a eventos de seguridad, mejorar la eficiencia y acelerar la automatización de las operaciones de seguridad. Para alcanzar el potencial de estas tecnologías, se necesita contar con procedimientos integrales que incluyan operaciones de seguridad y respuesta a incidentes, y que además estén en línea con los objetivos del negocio, adaptados a los riesgos particulares de la empresa y personalizados para la industria correspondiente y los procesos de administración empresariales y de servicios generales.

Si cuenta con un conjunto adecuado de procedimientos y un manual de ejecución operativo eficiente, la unificación de los procesos de respuesta a incidentes y las operaciones de seguridad con el enfoque de administración empresarial y de servicios puede convertir de manera eficaz la información y los posibles eventos de seguridad en medidas proactivas para eliminar las amenazas de seguridad o mejorar la respuesta ante posibles riesgos. Los procesos de administración eficientes favorecerán una administración útil de incidentes y aumentarán la eficiencia general de la administración de seguridad.

RSA®
The Security Division of EMC

Servicio de administración de operaciones de seguridad

El servicio Administración de operaciones de seguridad está diseñado para ayudar a las organizaciones con la alineación y la automatización estratégicas de creación de informes y procesos de seguridad, operaciones y cumplimiento de normas, y permitirles administrar un programa diario de manejo de incidentes. Mediante el desarrollo de procesos y procedimientos, este servicio alinea las metodologías y las estrategias operativas con los requisitos del negocio.

Actualmente, en muchas organizaciones se implementan tecnologías como la administración de eventos e incidentes de seguridad (SIEM) de manera táctica para enfrentar algún problema específico o simplemente como integrador de logs. Esta implementación limitada que incorpora logs de seguridad, sin soporte de procesos ni procedimientos, no permite aprovechar al máximo el potencial de la plataforma SIEM para reducir los riesgos y automatizar las operaciones de seguridad. Cuando SIEM se implementa de manera estratégica para enfrentar los retos críticos del negocio, es más fácil lograr una administración de seguridad consistente en toda la empresa y reducir los costos asociados con el cumplimiento de normas y la sobrecarga de TI. Al contar con una funcionalidad operativa integral, usted puede automatizar tantos procesos como sea posible para cumplir con los objetivos de seguridad y cumplimiento de normas, y mantener el personal necesario a un nivel reducido o el nivel existente.

Este servicio de RSA incrementa el ROI en operaciones de seguridad gracias a la definición de procesos y procedimientos eficientes, la centralización de actividades y la identificación de eficiencias de automatización que, de manera conjunta, garantizan la alineación con los impulsores del negocio y los objetivos generales. El servicio incluye el desarrollo de procesos y procedimientos de administración de seguridad, respuesta a incidentes, creación de informes de cumplimiento de normas y operaciones de TI. Por ejemplo, una revisión de la seguridad puede dar como resultado el desarrollo de planes para la automatización de aspectos del centro de operaciones de seguridad (SOC), como un sistema de tickets corporativos.

Dominio	Negocio			Operaciones			Infraestructura		
Componente de la plataforma	Métricas y medición	Uso funcional	Operación del negocio	Personal	Procedimientos	Administración de incidentes	Facilidades	TI	Seguridad
	Estrategia y evaluación *Acelere las funcionalidades en función de los objetivos del negocio y las mejores prácticas.* – Aprovecha la librería de casos de uso. – Estándares y metodologías de implementación demostrados, mejores prácticas.			**Administración** *Desarrolle u optimice los aspectos operativos de una función de administración de incidentes u operaciones de seguridad.* – Establece políticas, procedimientos, pautas y documentación. – Manuales de ejecución operativos y flujo de trabajo basados en mejores prácticas establecidas para operaciones de seguridad y data center.			**Análisis y diseño** *Amplio análisis de requisitos y diseño recomendado para operaciones de administración de incidentes y de seguridad eficientes.* – Análisis de requisitos: técnicos, operativos, de negocios. – Plan de trabajo de implementación y diseño recomendado basado en tecnología de RSA (SIEM, DLP como núcleo). – Arquitectura de referencia y marco de trabajo de manejo de incidentes.		

RSA Professional Services

Marco de trabajo de operaciones de seguridad

RSA Professional Services ofrece una serie de servicios de consultoría y asesoramiento destinada a satisfacer los requisitos de las empresas que desean desarrollar su función de operaciones de seguridad.

Alcance y enfoque

El servicio Administración de operaciones de seguridad comprende las estrategias de administración de seguridad, respuesta a incidentes, creación de informes de cumplimiento de normas y operaciones de TI:

- **Administración de seguridad:** proporciona una evaluación y un plan de trabajo para mejorar la administración de la seguridad de la información, y las operaciones y los procedimientos de manejo de incidentes. La contratación determina las amenazas y las prioridades para el manejo de incidentes en la organización. Esto hace posible la implementación de soluciones tecnológicas asociadas, por ejemplo SIEM, para proporcionar y crear una vista centralizada de la seguridad de la información y el manejo de incidentes para mejorar las operaciones e incrementar la eficiencia.
- **Personal:** identificación y desarrollo del modelo de recursos y personal; selección de personal y requisitos de capacitación, funciones y responsabilidades.
- **Respuesta a incidentes:** desarrollo de procesos y flujo de trabajo de administración de operaciones de seguridad para desarrollar, escalar y resolver incidentes y alertas.
- **Creación de informes sobre cumplimiento de normas:** considera las necesidades del negocio y los requisitos contractuales, legislativos y reglamentarios. Muestra dónde debe alinear los requisitos de cumplimiento de normas con los controles ISO 27002. Las recomendaciones incluyen procedimientos para automatizar los requisitos de creación de informes sobre cumplimiento de normas.
- **Procedimientos:** desarrollo de las políticas, los estándares y las pautas necesarios para el personal, junto con la documentación completa y un manual de ejecución operativo para la administración diaria.
- **Operaciones de TI:** proporciona una evaluación de las operaciones de TI y recomendaciones de automatización para mejorar las operaciones y la eficiencia. Por ejemplo, puede incluir planificación de capacidades, resolución de problemas, detección de fallas y eventos, centro de servicios y administración de incidentes, y performance. La contratación también lo ayuda a determinar la importancia de los componentes de la infraestructura y los requisitos de acceso a recursos de información.

Están basados en mejores prácticas, estándares y metodologías de implementación comprobados, por ejemplo estándares ISO, SANS y NIST para procedimientos de manejo de logs, administración de eventos y administración de incidentes. Los consultores de TI y seguridad de RSA descubren las funcionalidades actuales, registran el estado actual y alinean estos elementos con los objetivos del negocio. El informe final documenta las áreas que es necesario optimizar y en las que se puede mejorar la eficiencia por medio de la automatización de procesos.

RSA®
The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

©2009 RSA Security Inc. Todos los derechos reservados.
RSA, RSA Security y el logotipo de RSA son marcas registradas o marcas comerciales de RSA Security Inc. en los Estados Unidos y en otros países. EMC es una marca registrada de EMC Corporation. Todos los demás productos y servicios mencionados son marcas registradas de sus respectivas empresas.

SOCMG DS 1009